

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of:

FRANCIS X. McKEEN, ET AL.

Application No.: 09/672,367

Filed: September 28, 2000

For: **A MECHANISM TO SECURE  
COMPUTER OUTPUT FROM  
SOFTWARE ATTACK USING  
ISOLATED EXECUTION**



Art Group: 2134

Examiner: Thomas M. Ho

INFORMATION DISCLOSURE STATEMENT UNDER 37 C.F.R. § 1.97

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**RECEIVED**

JUN 14 2004

Technology Center 2100

In accordance with the duty of disclosure, enclosed is a copy of IDS Citation Form PTO/SB/08 or PTO-1449, together with copies of the documents cited on that form, except for copies not required to be submitted (e.g., copies of U.S. patents and U.S. published patent applications need not be enclosed for applications filed after June 30, 2003). This IDS and IDS Citation Form are being submitted before the mailing of a final Office Action. It is respectfully requested that the cited references be considered and that the enclosed copy of PTO/SB/08 be initialed by the Examiner to indicate such consideration and a copy thereof returned to applicant(s).

**BEST AVAILABLE COPY**

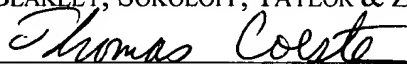
The submission of this Information Disclosure Statement is not to be construed as a representation that a search has been made in the subject application and is not to be construed as an admission that the information cited in this statement is material to patentability.

Applicant has concurrently submitted an electronic Information Disclosure Statement(s). Any fees that are required for submission of an Information Disclosure Statement were included in the electronic submission. Applicant respectfully requests that one submitted fee be accepted for the second and any subsequent Information Disclosure Statement submissions. The fee set in the amount of \$180.00 for submission of the Information Disclosure Statement is enclosed herewith. Please charge any additional fees due to Deposit Account 02-2666. A duplicate copy of the Fee Transmittal (PTO/SB/17) is enclosed for this purpose.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: June 02, 2004



Thomas M. Coester, Reg. No. 39,637

12400 Wilshire Boulevard, 7th Floor  
Los Angeles, CA 90025  
Telephone: (310) 207-3800

I hereby certify that this correspondence is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.



Susan M. Barrette

06-02-04

Date

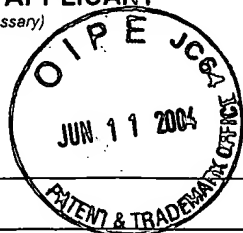
**BEST AVAILABLE COPY**

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**

(Use as many sheets as necessary)



Complete if Known

|                      |                    |
|----------------------|--------------------|
| Application Number   | 09/672,367         |
| Filing Date          | September 28, 2000 |
| First Named Inventor | Francis X. McKeen  |
| Group Art Unit       | 2134               |
| Examiner Name        | Thomas M. Ho       |

Sheet 1 of 3

Attorney Docket No: 042390.P9578

**US PATENT DOCUMENTS**

| Examiner Initial * | USP Document Number | Publication Date | Name of Patentee or Applicant of cited Document | Class | Subclass | Filing Date If Appropriate |
|--------------------|---------------------|------------------|-------------------------------------------------|-------|----------|----------------------------|
|--------------------|---------------------|------------------|-------------------------------------------------|-------|----------|----------------------------|

**FOREIGN PATENT DOCUMENTS**

| Examiner Initials* | Foreign Document No | Publication Date | Name of Patentee or Applicant of cited Document | Class | Subclass | T <sup>2</sup> |
|--------------------|---------------------|------------------|-------------------------------------------------|-------|----------|----------------|
|                    | DE-4217444          | 12/03/1992       | Toyohisa, Imada, et al.                         |       |          |                |
|                    | EP-0473913          | 03/11/1992       | Farrell, Joel A.                                |       |          |                |
|                    | EP-0600112          | 06/08/1994       | Wimmer, Manfred D.                              |       |          |                |
|                    | EP-0930567          | 07/21/1999       | Brewer, Jason M.                                |       |          |                |
|                    | EP-0961193          | 12/01/1999       | Laczko, Sr., Frank L.                           |       |          |                |
|                    | EP-0965902          | 12/22/1999       | Force, Gordon, et al.                           |       |          |                |
|                    | EP-1030237          | 08/23/2000       | Proudlar, John, et al.                          |       |          |                |
|                    | EP-1085396          | 03/21/2001       | Proudlar, Graeme J., et al.                     |       |          |                |
|                    | EP-1146715          | 10/17/2001       | Wang, Xin, et al.                               |       |          |                |
|                    | EP-1271277          | 01/02/2003       | Behar, Yaachov                                  |       |          |                |
|                    | JP-2000076139       | 03/14/2000       | Tanno, Masaaki, et al.                          |       |          |                |
|                    | WO-0021238          | 04/13/2000       | Drews, Paul C.                                  |       |          |                |
|                    | WO-0062232          | 10/19/2000       | Headrick, Samuel P., et al.                     |       |          |                |
|                    | WO-0127723          | 04/19/2001       | Vamvakas, Athanasia, et al.                     |       |          |                |
|                    | WO-0127821          | 04/19/2001       | Chen, Ligu, et al.                              |       |          |                |
|                    | WO-0163994          | 08/30/2001       | Van Sant, Glen, et al.                          |       |          |                |
|                    | WO-0175564          | 10/11/2002       | Herbert, Howard C., et al.                      |       |          |                |
|                    | WO-0175565          | 10/11/2001       | Ellison, Carl M.                                |       |          |                |
|                    | WO-0175595          | 10/11/2001       | Ellison, Carl M., et al.                        |       |          |                |
|                    | WO-02086684         | 10/31/2002       | Proudlar, Graeme J.                             |       |          |                |
|                    | WO-0217555          | 02/28/2002       | Ford, Warwick                                   |       |          |                |
|                    | WO-9524696          | 09/14/1995       | Mooney, David M., et al.                        |       |          |                |
|                    | WO-9729567          | 08/14/1997       | Gressel, Carmi, et al.                          |       |          |                |
|                    | WO-9834365          | 08/06/1998       | Devanbu, Premkumar T., et al.                   |       |          |                |
|                    | WO-9844402          | 10/08/1998       | Bramhill, Ian D., et al.                        |       |          |                |
|                    | WO-99/65579         | 12/23/1999       | Bond, Eugene T.                                 |       |          |                |
|                    | WO-9905600          | 02/04/1999       | Garst, Blaine, et al.                           |       |          |                |
|                    | WO-9909482          | 01/15/2002       | Bausch, Jean                                    |       |          |                |
|                    | WO-9957863          | 11/11/1999       | Hayes Jr., Kent F., et al.                      |       |          |                |

RECEIVED

JUN 14 2004

Technology Center 2100

**OTHER DOCUMENTS -- NON PATENT LITERATURE DOCUMENTS**

EXAMINER

**BEST AVAILABLE COPY**

DATE CONSIDERED

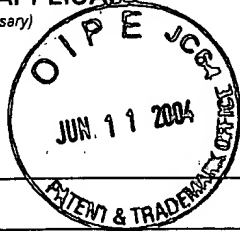
Substitute Disclosure Statement Form (PTO-1449)

\* EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. 1 Applicant's unique citation designation number (optional) 2 Applicant is to place a check mark here if English language Translation is attached

Substitute for form 1449A/PTO

# INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)



Complete if Known

Application Number 09/672,367  
Filing Date September 28, 2000  
First Named Inventor Francis X. McKeen  
Group Art Unit 2134  
Examiner Name Thomas M. Ho

RECEIVED

JUN 14 2004

Sheet 2 of 3

Attorney Docket No: 042390.P9578

Technology Center 2100

| Examiner Initials* | Cite No. | Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.                          |  |
|--------------------|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
|                    |          | BERG, CLIFF, "How Do I Create a Signed Applet?", <u>Dr. Dobb's Journal</u> , (08/1997), 1-9                                                                                                                                                                                              |  |
|                    |          | BRANDS, STEFAN, "Restrictive Binding of Secret-Key Certificates", <u>SPRINGER-VERLAG XP002201306</u> , (1995), Chapter 3                                                                                                                                                                 |  |
|                    |          | CHIEN, ANDREW A., et al., "Safe and Protected Execution for the Morph/AMRM Reconfigurable Processor", <u>7th Annual IEEE Symposium, FCCM '99 Proceedings</u> , XP010359180, ISBN 0-7695-0375-6, Los Alamitos, CA, (4/21/1999), 209-221                                                   |  |
|                    |          | COMPAQ COMPUTER CORPORATION, et al., "Trusted Computing Platform Alliance (TCPA) Main Specification Version 1.1a", (12/2001), 1-321                                                                                                                                                      |  |
|                    |          | DAVIDA, GEORGE I., et al., "Defending Systems Against Viruses through Cryptographic Authentication", <u>Proceedings of the Symposium on Security and Privacy</u> , IEEE Comp. Soc. Press, ISBN 0-8186-1939-2, (May 1989),                                                                |  |
|                    |          | GOLDBERG, ROBERT P., "Survey of Virtual Machine Research", <u>COMPUTER Magazine</u> , (06/1974), 34-35                                                                                                                                                                                   |  |
|                    |          | GONG, LI, et al., "Going Behind the Sandbox: An Overview of the New Security Architecture in the Java Development Kit 1.2", <u>Proceedings of the USENIX Symposium on Internet Technologies and Systems</u> , Monterey, CA, (12/1997),                                                   |  |
|                    |          | GUM, P. H., "System/370 Extended Architecture: Facilities for Virtual Machines", <u>IBM J. Research Development</u> , Vol 27, Number 6, (11/1983), 530-544                                                                                                                               |  |
|                    |          | HEINRICH, JOE, "MIPS R4000 Microprocessor User's Manual, Second Edition", Chapter 4 "Memory Management", (6/11/1993), 61-97                                                                                                                                                              |  |
|                    |          | IBM, "Information Display Technique for a Terminate Stay Resident Program IBM Technical Disclosure Bulletin", <u>TDB-ACC-No. NA9112156</u> , Vol. 34, Issue 7A, (12/1/1991), 156-158                                                                                                     |  |
|                    |          | INTEL, "IA-32 Intel Architecture Software Developer's Manual", <u>Volume 3: System Programming Guide</u> , Intel Corporation - 2003, 13-1 through 13-24                                                                                                                                  |  |
|                    |          | INTEL, "Intel386 DX Microprocessor 32-Bit CMOS Microprocessor With Integrated Memory Management", (1995), 5-56                                                                                                                                                                           |  |
|                    |          | KARGER, PAUL A., et al., "A VMM Security Kernel for the VAX Architecture", <u>Proceedings of the Symposium on Research in Security and Privacy</u> , XP010020182, ISBN 0-8186-2060-9, Boxborough, MA, (5/7/1990), 2-19                                                                   |  |
|                    |          | KASHIWAGI, KAZUHIKO, et al., "Design and Implementation of Dynamically Reconstructing System Software", <u>Software Engineering Conference</u> , Proceedings 1996 Asia-Pacific Seoul, South Korea 4-7 Dec. 1996, Los Alamitos, CA USA, IEEE Comput. Soc. US, ISBN 0-8186-7638-8, (1996), |  |
|                    |          | LAWTON, KEVIN, et al., "Running Multiple Operating Systems Concurrently on an IA32 PC Using Virtualization Techniques", <u>http://www.plex86.org/research/paper.txt</u> , (11/29/1999), 1-31                                                                                             |  |
|                    |          | LUKE, JAHN, et al., "Replacement Strategy for Aging Avionics Computers", <u>IEEE AES Systems Magazine</u> , XP002190614, (March 1999),                                                                                                                                                   |  |

EXAMINER

BEST AVAILABLE COPY

DATE CONSIDERED

Substitute Disclosure Statement Form (PTO-1449)

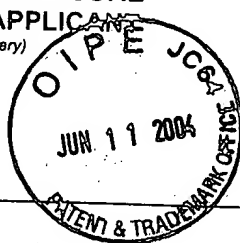
\* EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional) 2 Applicant is to place a check mark here if English language Translation is attached

Substitute for form 1449A/PTO

# INFORMATION DISCLOSURE

## STATEMENT BY APPLICANT

(Use as many sheets as necessary)



Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Approved for use through 10/31/2002. OMB 651-0031  
US Patent & Trademark Office: U.S. DEPARTMENT OF COMMERCE

Complete if Known

|                      |                    |
|----------------------|--------------------|
| Application Number   | 09/672,367         |
| Filing Date          | September 28, 2000 |
| First Named Inventor | Francis X. McKeen  |
| Group Art Unit       | 2134               |
| Examiner Name        | Thomas M. Ho       |

Sheet 3 of 3

Attorney Docket No: 042390.P9578

## OTHER DOCUMENTS -- NON PATENT LITERATURE DOCUMENTS

| Examiner Initials* | Cite No. <sup>1</sup> | Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published. | T <sup>2</sup> |
|--------------------|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
|                    |                       | MENEZES, OORSCHOT, "Handbook of Applied Cryptography", CRC Press LLC, USA XP002201307, (1997),475                                                                                                                                                               |                |
|                    |                       | MOTOROLA, "M68040 User's Manual", (1993),1-1 to 8-32                                                                                                                                                                                                            |                |
|                    |                       | RICHT, STEFAN, et al., "In-Circuit-Emulator Wird Echtzeittauglich", Elektronik, Franzis Verlag GMBH, Munchen, DE, Vol. 40, No. 16, XP000259620,(100-103),8-6-1991                                                                                               |                |
|                    |                       | ROBIN, JOHN S., et al., "Analysis of the Pentium's Ability to Support a Secure Virtual Machine Monitor", Proceedings of the 9th USENIX Security Symposium, XP002247347, Denver, Colorado, (8/14/00),1-17                                                        |                |
|                    |                       | ROSENBLUM, M., "Virtual Platform: A Virtual Machine Monitor for Commodity PC", Proceedings of the 11th Hotchips Conference, (8/17/1999),185-196                                                                                                                 |                |
|                    |                       | SAEZ, SERGIO, et al., "A Hardware Scheduler for Complex Real-Time Systems", Proceedings of the IEEE International Symposium on Industrial Electronics, XP002190615,(July 1999),43-48                                                                            |                |
|                    |                       | SHERWOOD, TIMOTHY, et al., "Patchable Instruction ROM Architecture", Department of Computer Science and Engineering, University of California, San Diego, La Jolla, CA, (Nov. 2001),                                                                            |                |

RECEIVED

JUN 14 2004

Technology Center 2100

EXAMINER

BEST AVAILABLE COPY

DATE CONSIDERED